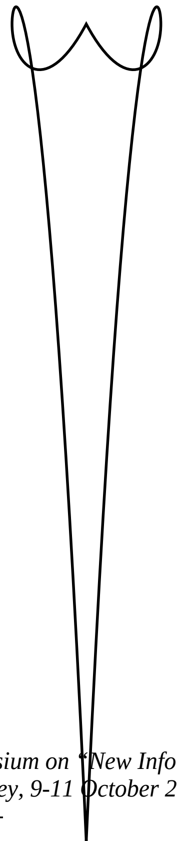


Paper presented at the RTO IST Symposium on "New Information Processing Techniques for Military Systems",
held in Istanbul, Turkey, 9-11 October 2000, and published in RTO MP-049.

Copenhagen school: "Don't ask, just do the math!" Many physicists disparage my favorite, the Multiple Universes (Multiverse) Theory, but some show its simplicity[4]. We sometimes cannot know what really did happen, simply because Nature forgot. Nevertheless, we all assume the past is unique in most of our thinking. We soon forget what we had for lunch a week ago, but we are confident that the answer is unambiguous. The exact number of carbon atoms we ingested may be ambiguous, and we have no way of knowing exactly what the course of events (or food) really was. We live in a world of approximations. The past may not be unique. What other unwarranted assumptions do we blithely make?

> That mathematicians throughout the ages should have made various mistakes about matters of proof and certainty is only natural. The present discussion should lead us to expect that the current view will not last forever, either. But the confidence with which mathematicians have blundered into these mistakes and their inability to acknowledge even the possibility of error in these matters are, I think, connected with and ancient and widespread confusion between the *methods* of mathematics and its *subject-matter*. -- David Deutsch[4].

What's a Qubit?: We can replace the photons in the two-slit experiment with electrons, protons, atoms, even buckeye-balls, and still get a diffraction pattern. Similar ambiguities in Nature result from other phenomena, such as the polarization of light and the spins of subatomic particles. These spins can be controlled by resonant microwave radiation. Any such ambiguity can be exploited to construct a quantum bit or 'qubit', which is like a conventional bit in that it can store one of two states, except that a qubit can store a mixture of two states as long as we do not know which state it stores. When it is observed, a qubit assumes one of the two states.

Quantum Computers: A quantum computer is a device that exploits qubits (however constructed) to explore several possibilities at the same time with the same hardware. Williams and Clearwater[8] have explained the theory well. Whereas one qubit has a superposition of two states, two qubits have a superposition of four states, three qubits have a superposition of eight states, and so on, so that N qubits have a superposition of 2^N states. The qubits can maintain this superposition without interacting with each other as long as outside forces do not disrupt the coherence.

NMR Quantum Computers: Quantum computers can be built in several ways, and ultimately in ways not yet considered. Nuclear magnetic resonance (NMR) has been used to build some of the first functional quantum computers. The idea is that each molecule in a solution is a quantum computer with some of its atoms constituting the qubits. For example, alanine has three carbon atoms, which can be replaced by carbon-13 atoms with spin $^1/_2$. Measuring the spins of these atoms in a strong magnetic field will show them aligned either with or against the magnetic field. Each atom in the molecule has a resonance frequency, and applying resonant microwave radiation at that frequency can modify its spin. All the atomic spins normally precess in their local magnetic fields as affected by the spins of neighboring atoms. An NMR quantum computer program therefore consists of a sequence of microwave pulses at specified frequencies and in specified directions each followed by a delay of a specified duration to allow coupling between qubits.

Quantum Algorithms: Researchers have developed four algorithms for quantum computers. Williams and Clearwater[8] explain these algorithms in detail. Feynman[9] predicted that physics could be simulated on a quantum computer more readily than on a conventional computer. Recent developments in quantum harmonic oscillators[10] show how practical Feynman simulators might develop. The Shor Algorithm[11] shows in principle how to factor large numbers quickly (but no quantum computer has yet factored 15). Grover's Algorithm[12] shows how to search unstructured databases, with modest success in searching a four-bit database. The Deutsch-Jozsa Algorithm[13] shows how to measure a global property of a function (such as whether a predicate of a four-bit number is constant or true on half of all possible inputs) by executing it on all possible inputs simultaneously.

Entanglement: The notion of entangled qubits is currently a hot topic[14] and is likely to lead to improvements in communications technology. Some sophisticated experiments[15] have shown that two particles with correlated quantum states can maintain their correlation over great separation distances. Entanglement happens whenever a system can exist in a superposition of just some of the possible states. For example, three qubits are entangled if they could never be observed in the same state; that is, one must differ from the other two. If the state of a qubit is not determined until it is measured, how can one qubit know that the other two have the same state? Although entanglement is not required in all quantum algorithms, it may be very important in building large quantum computers. Eventually entanglement may be used to communicate quantum states between widely separated parts of a networked quantum computer.

Bit-Parallel Algorithms: Some algorithms for quantum computers, including the Deutsch-Josza Algorithm, work like bit-parallel algorithms. For example, a 5-bit input has 32 possible values, so we assign a bit position in a 32-bit word to each of those values. Every possible predicate of that input corresponds to some 32-bit signature. To negate a predicate, complement its signature. To require all of several predicates, take the logical intersection (and) of their signatures. To require any of several predicates, use logical union (or), These operations can be carried out in parallel for all possible 5-bit inputs. To evaluate a predicate for any specific 5-bit input, just look at the corresponding bit of the signature of the predicate.

Complexity: The complexity of a problem is the scale of its difficulty measured as the growth rate of the logistical resources required to solve it as a function of the size parameters of the problem. We do not need to be overly specific here, and we especially do not need to define terms like NP-complete. A simple scale is enough (see Fig. 2):

- Easy -- a solution costs pennies, you do it yourself;
- Nontrivial -- a solution costs dollars, you buy it;
- Hard -- a solution requires research, someone learns something;
- Intractable -- costs double for a fixed increase in size, versus a tractable problem for which costs double for some percentage increase in size.
- Noncomputable -- there is proof that no general solution is possible.

Turing Tarpit: Theorems about limits on what can be done have a chilling effect on research. Teach a bright student about Turing noncomputability (proofs that some functions are inherently not computable on conventional computers) and that student will later recognize certain problems as being noncomputable and not even try, although partial solutions could be extremely valuable. He appears to be mired in the Turing Tarpit[16] and the deeper one's understanding, the harder it is to ignore limits. For example, we know that there cannot be a proof procedure that determines whether an arbitrary program ever terminates, but we can design proof procedures that work on a class of programs large enough to include all acceptable programs by definition. Reliable programs tend to be simple. For another example, a recent paper[17] claims that NMR quantum computers as currently constructed cannot demonstrate entanglement. The paper does not refute the assumption that each molecule in solution in an NMR computer attains all its allowed states simultaneously, but shows that the approximations used in small NMR quantum computers do not demonstrate entanglement. We cannot expect to escape the Turing Tarpit by shallow thinking. We need to understand all the assumptions that determine various limits.

Tractability: Quantum computers and conventional computers can theoretically simulate each other. Therefore what is not computable for one is not computable for the other. Quantum computers have an exponential advantage however; so what will always be intractable for a conventional computer may become tractable for a quantum computer. A tractable problem is theoretically practical. We turn hard problems into nontrivial problems through research, and nontrivial problems into easy problems through education.

Grand Challenges: The Office of Naval Research has posted four Grand Challenges[18], problem areas that the Navy currently sees as very significant:

- Battle Space Awareness
- Naval Materials by Design
- Electric Power Sources
- Intelligent Naval Sensors

Quantum computers and related technology may someday contribute substantially to these challenges. They are likely to contribute to meeting the first three challenges through improved simulators. Intelligent naval sensors will benefit most when quantum computers help artificial intelligence succeed. Artificial intelligence may be the ultimate beneficiary of quantum computing because many of its failures have resulted from the intractability of the problems it faced.

Moore's Law: Many charts show the dramatic exponential growth of computer technology throughout its history. Gordon Moore predicted that this growth in 1963 when he had only three data points. He has since said that his rule was not a law, but a self-fulfilling prophecy[19]. The silicon industry adopted Moore's Law as a guideline in establishing an industry roadmap[20]. Manufacturers who were behind the curve had to allocate more resources to stay competitive, but those who were ahead could relax a little. Many progress charts have been prepared and are available on the web. One of the best charts[21] shows the evolution of computer power over cost compared to evolution of human brainpower.

Limits: Moore's Law cannot continue to hold for conventional computers. The speed of light, the Heisenberg Uncertainty Principle, and the Rayleigh Resolution Criterion limit conventional computers. Quantum computers hold forth the possibility of side stepping these limits by performing computations in many parallel universes simultaneously. The various limits do not constrain the computation until a measurement is attempted. We do not know what other limits will be discovered on quantum computation.

Imagery: How could a quantum computer use its enormous state space? That depends on the kinds of data structures that are developed for quantum computers. For example, a 2^Ax2^B-pixel image could be mapped through Fock-state preparation[22] onto the superposed states of A+B qubits. Specifically, one HDTV screen image (1024x1024 pixels) could be mapped onto 20 qubits, and a four-hour movie (2^{14} seconds) at 64 frames per second could be mapped onto 40 qubits. That is not to say that we could get the images back again because a quantum computer with N qubits will only be able to answer N yes/no questions. That problem is partially addressed by using a great number (say 10^{18}) of very small (molecular) quantum computers running the same program. Even so, the state space grows much faster with additional qubits than the possibility of deploying enough quantum computers to render the quantum state on a conventional computer. For example, just 700 qubits would be enough to map a Euclidean universe the size and duration of our own down to the Planck scale (10^{-35} cm). There would be a substantial input/output problem.

Processing: The problem is not how to extract the quantum state from the qubits, but how to process mapped images so much simpler questions can be answered. The assumption necessary for exploiting quantum computers is that each quantum computer assumes all of its allowed states in each run. The initial and final states may be small, but the computation may proceed through an extremely large intermediate state space that is not measured. For example, could a quantum computer locate an image of a face or a weapon in a collection of a thousand one-hour movies? The answer needs 10 bits to say which movie plus 18 bits to say which frame, not the 2^{20} bits needed to render that frame. For another example, a quantum computer should be able to simulate certain physical systems, such as the weather or the propagation of underwater sound. I say 'should' for sound (and radar) because the various wave equations are time symmetric up to the inclusion of attenuation, and I have run such simulations backwards[23]. The fundamental operations of a quantum computer are unitary (time symmetric) transformations, except for making observations, starting up, and shutting down. These exceptions prove that the full operation of a quantum computer need not be time symmetric. Time symmetry is just a means of improving performance.

Education: Quantum computers will help solve many interesting and worthwhile problems only when enough researchers have the tools and expertise to tackle them. Not only will these researchers have to master their problem domains, they will have to understand and rework the assumptions in those domains. Nahin did so for time travel[24] by his scholarly and comprehensive analysis of our assumptions about time. The purpose of many assumptions is to make certain solutions tractable. Any technology that changes what is tractable will require re-examination of the underlying assumptions of any field that might use that technology. We must not only train future researchers to use basic techniques, but to invent them. We must also assume that productive programming environments for general-purpose quantum computers can be developed. Having quantum computers that are accessible most of the time will greatly contribute to the education of many experts in programming them.

Direction: We need a reference point for future analysis, a design that is well ahead of the state of the art, so that we can make future estimates about the development of quantum computers. To freeze the reference point, we will use a very old design[25], one that will not change because it has not changed. The Rabi Quantum Computer is named after Isador Isaac Rabi, an Austrian-born American physicist who discovered that resonant microwave radiation could affect the spins of subatomic particles. It is specified to be 300 qubits long, 50 qubits wide, and 30 qubits high with a 1 qubit high grid on top for an interface to a windows system (see Fig. 3). This design could help us survive an information flood that makes our current one look like an April shower. It could surely take on the complete genome for two of every kind of animal in the world, because it is the RQC (pronounced "ark, you see" in English). However, the imminent use of this design does not depend on actually building it or on faith in its Designer, but on its uncontested age, so that an estimate of when it could be constructed will be commensurate with future estimates.

Schedule: When could an RQC be built? Current estimates are necessarily very vague. We need to progress from the current state of the art of short linear 8-qubit chains to large chains and grids. Some sixteen doublings are required to build the RQC as specified with 450000 ~ $8*2^{16}$ qubits. I expect the following stages will take place:

1-2 years:	QC concepts proven;
2-5 years:	Some QC is up all the time;
5-10 years:	Remote QC access for study;
10-25 years:	Practical QC grids available;
25-50 years:	Cheap QC’s in use everywhere;
50-100 years:	An RQC can be built.

Shortcuts: Advances in technology sometimes take surprising leaps when supporting technology is available. Perhaps someone will figure out how to exploit the magnetic fields in old core memories to control qubit grids. Perhaps someone will couple CCD grids (as in camcorders) to qubit grids, so that a complicated quantum computer program can be prepared as a video clip. An RQC could conceivably be built in twenty years. At least by then we will have 2020 hindsight.

Connections: Although a linear chain of qubits is enough because the quantum states of two adjacent qubits can be exchanged, more complicated networks are probably desirable. There are indications even now that we will be able to create three-dimensional qubit grids using DNA structures[26]. How those qubits are interconnected is not specified. Connecting each qubit to its six nearest neighbors is surely overkill. Connecting 15000 chains of 50 qubits to 300 chains of 30 qubits in the I/O grid, each connected to one chain of 50 qubits may be awkward because moving quantum states around such a network may lose many of the benefits obtained from quantum computing.

Perfect Shuffle: A connection topology that has minimal direct connections for easy implementation and maximal indirect connections for rapid movement of quantum states will be desirable. One perfect shuffle network (see Fig. 4) connects each cell directly with just three other cells, but indirectly with some 2^k cells in k steps. For an example that does not quite meet the RQC specification, consider connecting M=131071 cells in loops of P=17 cells each with the remaining cell linked to itself. Number the cells in one such collection so that cell n is connected to cell 2n (modulo M). Number the cells in another such collection so that cell n is connected to cell 2n+1 (modulo M). Entangling qubits in correspondingly numbered cells from each collection creates a perfect shuffle network. All M cell pairs are connected in a single long chain by uniform sequences of steps (back-shuffle-forward-shuffle). Other uniform sequences of steps connect distant parts of that long chain. To get halfway around the chain (π=65576), use a different step sequence (forward-shuffle-back-shuffle). Every cell is connected to just three cells, but has a tree of all other cells both below it and above it. This would be great for artificial intelligence applications, which are frequently recursive.

Stimulation: An ulterior purpose of the design of the RQC is to stimulate imaginations. The more researchers dream about the possibilities in the exponential potential of quantum computers, the sooner quantum computers can be profitably applied to real problems. What might the future bring?

My Dreams: I hope that this paper will help liberate the imaginations of many students who will help other students learn to make quantum computers useful in many fields. I also want to persuade the National Oceanic and Atmospheric Administration (NOAA) to focus its efforts in Quantum Computing by adopting a long-range goal of building the RQC for use in weather forecasting. ☺

References:

[1] Harold A. Linstone, *Murray Turoff, The Delphi Method,* Addison-Wesley Publishing Co. (Reading MA) ©1975; ISBN 0-201-04294-0, ISBN 0-201-04293-2 pbk.

[2] Ibid., p.374.

[3] Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World,* Doubleday (New York) ©1991, 1996.

[4] David Deutsch, The Fabric of Reality, The Penguin Press (New York) ©1997.

[5] Etienne Klein, *Conversations with the Sphinx: Paradoxes in Physics,* Souvenir Press (London), translated 1996; ISBN 0 285 63305 8 (hardback).

[6] D. Halliday, R. Resnik, K. Krane, *Physics, Volume Two, Extended Version,* Fourth Edition, John Wiley & Sons (New York) ©1992; p.1064.

[7] Gerald P. Milburn, *The Feynman Processor,* Perseus Books (Reading MA) ©1998; p.20 citing Feynman.

[8] Colin P. Williams, Scott H. Clearwater, *Explorations in Quantum Computing,* Springer TELOS ((Santa Clara CA) ©1998; ISBN 0-387-94768-X.

[9] Richard P. Feynman, "Simulating Physics with Computers", *International Journal of Theoretical Physics,* vol. 21, nos. 6/7, 1982, pp. 467-488.

[10] C.R. Nave, "Quantum Harmonic Oscillator", Georgi State University; http://230nsc1.phy-astr.gsu.edu/hbase/quantum/hosc.html

[11] P W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos CA, a994), pp. 124-134.

[12] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", *Phys. Rev. Lett.* **79**, 325 (1997).

[13] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal, "NMR Quantum Computation with Indirectly Coupled Gates", *e-print* quant-ph/9910006.

[14] Michael Brooks (ed.), *Quantum Computing and Communications,* Springer-Verlag (London, …) ©1999; ISBN 1-85233-091-0.

[15] Ibid., p.123.

[16] A.J. Perlis, *personal communications,* circa 1970; there is no consensus as to what Perlis meant by the Turing tarpit.

[17] R. Fitzgerald, "What really gives a quantum computer its power?" , *Physics Today,* 2000 Jan, pp.20-22.

[18] Office of Naval Research, "S&T Grand Challenges", http://www.onr.navy.mil /sci_tech/chief/GrandChal.htm

[19] Gordon Moore, (speech), 50th Anniversary of the ACM, 1997.

[20] (a global community of researchers, manufacturers, and suppliers), *International Technology Roadmap for Semiconductors: 1999 Edition,* Semiconductor Industry Association (San Jose CA) 1999; http://notes.sematech.org/ntrs/PublNTRS.nsf/

[21] Jeff Sutherland, "Evolution of Computer Power/Cost", http://www.jeffsutherland.org/objwld98/future.html

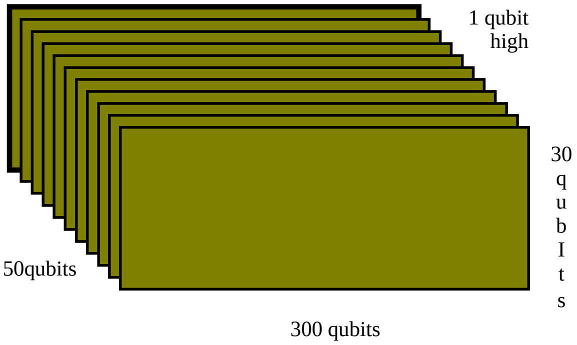
[22] G. Harel and G. Kurizki, “Fock-State Preparation from Thermal Cavity Fields by Measurements on Resonant Atoms”, *Phys. Rev. A.* 54, 5410 (1996).

[23] R. A. Krutar, S. K. Numrich, et al., “Computation of Acoustic Field Behavior Using a Lattice Gas Model,” *Proc. Oceans 91 Conference* (Honolulu, 1991), Vol. 1, pp. 446-452, IEEE.

[24] Paul J. Nahin, *Time Machines: Time Travel in Physics, Metaphysics, and Science Fiction,* Springer-Verlag (New York) ©1999, 1993; ISBN 0-387-98571-9.

[25] *Genesis* 6:14-16.

[26] C. Wu, "DNA Strands Connect the Quantum Dots", *Science News,* vol. 156, no, 12, 1888 Sep 16.


1 qubit
high
30 qubIts
50qubits
300 qubits

This page has been deliberately left blank

Page intentionnellement blanche